The following listing of claims replaces all prior versions and listing of claims in the application.

LISTING OF CLAIMS

1 – 18. (previously cancelled)

19. (previously added and now amended) A system for ciphering a packet in a data [~~for transmission~~] stream received by a communication device, said system comprising:

a first communication port for receiving said data stream;

a second communication port for transmitting a ciphered data stream associated with said data stream;

a memory device having

a memory buffer;

a first access port connected to said memory buffer; and

a second access port connected to said memory buffer; [~~and~~]

a data processing processor connected to said first communication port, said second communication port and said first access port via a first bus;

and

a ciphering processor connected to said second access port via a second bus,

wherein said first access port and said second access port each provide [~~mutually independent~~] access to said memory buffer; [~~said second bus is not connected to said first bus~~] said data processing processor is adapted to receive said data [~~and provide said data to~~] stream from said first communication port through said first bus, to identify a start and an end of said packet, to store a file associated with said packet in said memory buffer [~~over~~] through said first bus and to retrieve said ciphered data from said memory buffer through said first bus for transmission through said second communication port; and said ciphering processor is adapted to retrieve said [~~data~~] file from said memory buffer over said second bus, to generate said ciphered

data stream from said [~~data~~] file, to generate integrity check information for said ciphered data stream using contents of said [~~data~~] file and to provide said ciphered data stream to said memory buffer [~~over~~] through said second bus.

20. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim 19, wherein said ciphering processor includes an encryption module for generating said ciphered data stream and a hashing module for generating said integrity check information.

21. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim 19, wherein said ciphering processor includes an encryption module for generating said ciphered data stream and a [~~message digesting~~] module for generating said integrity check information.

22. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim 20, wherein said encryption module includes a DES encryption module for performing one of DES and triple-DES encryption.

23. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim 20, wherein said hashing module includes a HMAC hashing module for encoding said integrity check information within said ciphered data stream.

24. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim 19, wherein said memory buffer comprises dual port random access memory.

25. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim 19, wherein said data processing processor comprises a security module,

[~~said security module retrieves~~] adapted to retrieve a security context from memory [~~, said security context used~~] for use in generating said ciphered data stream.

26. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim 25, wherein said security module determines a security context relating to at least one of a source of said data stream and a destination for said ciphered data stream and stores said security context in said memory buffer, said security context stored being accessible by said ciphering processor.

27. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim 26, wherein said data processing processor comprises a security address module, said security address module stores an address associated with said security context in said memory buffer, said address based on said at least one of said source of said data stream and said destination for said ciphered data stream.

28. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim 25, wherein said security module provides an indication to said data processing processor when a security context is not present in said memory buffer.

29. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim 19, wherein said data processing processor operates asynchronously to said ciphering processor.

30. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim 29, wherein said data processing processor is clocked by a first clock source,

said ciphering processor is clocked by a second clock source and said first clock source is asynchronous to said second clock source.

31. (cancelled)

32. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim [31]30, wherein said data stream received at said first communications port comprises fragments of a packet, said data processing processor stores said fragments in said memory buffer to assemble said packet and said ciphering processor generates said ciphered data stream from said assembled packet.

33. (previously added and now amended) The system for ciphering a packet in a data stream as claimed in claim 32, wherein said system is disposed at a gateway between a private network and a public network in a secure virtual private network, said first communications port is connected to one of said private network and said public network and said second communications port is connected to another one of said private network and said public network.

34. (new) A method for ciphering a packet in a data stream received by a communication device having a first communication port for receiving said data stream, a second communication port for transmitting a ciphered data stream associated with said data stream, a memory device including a memory buffer and a first and a second access ports connected to said memory buffer, said communication device further having a data processing processor connected to said first communication port, said second communication port and said access port via a first bus and a ciphering processor connected to second access port via a second bus, said method comprising:

receiving said data stream from said first communication port for processing by said data processing processor;

identifying a start and an end of said packet by said data processing processor;

storing a file associated with said packet in said memory buffer by said data processing processor through said first bus;

retrieving said file from said memory buffer by said ciphering processor over said second bus;

generating said ciphered data stream from said file by said ciphering processor;

generating integrity check information for said ciphered data stream using contents of said file by said ciphering processor; and

providing said ciphered data stream to said second communication port.

35. (new) The method for ciphering a packet in a data stream as claimed in claim 34, said method further comprising,

retrieving a security context from memory for use in generating said ciphered data stream;

determining a security context relating to at least one of a source of said data stream and a destination for said ciphered data stream; and

storing said security context in said memory buffer, said security context stored being accessible by said ciphering processor.

* * *